
Security and Privacy in RFID

Aveiro Julio 2008



21/4/08 Brussels

Page 1



The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information as its sole risk and liability.

- Security and Privacy threats in RFID
- Privacy
- Authentication
- Basic RFID tags
- Privacy solutions basic tags: Killing and sleeping
- Privacy solutions basic tags: Renaming
- Privacy solutions basic tags: Proxying
- Privacy solutions basic tags: Distance measurement

Outline

- Privacy solutions basic tags: Blocking
- Authentication

Security and Privacy threats in RFID

- As any wireless technology, RFID is vulnerable to several kinds of security and privacy threats.
- The fact that intruders are able to read information freely from any tag poses an important privacy concern in RFID.
- There are many methods to greatly reduce such threats.
- However, intruders are always looking for innovative methods to overcome any security measure.

- RFID raises two main privacy concerns for users: *clandestine tracking and inventorying*.
- RFID tags respond to reader interrogation without alerting their owners or bearers. Thus, where read range permits, clandestine scanning of tags is a plausible threat.
- A person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for clandestine physical tracking.
- The threat to privacy grows when a tag serial number is combined with personal information

- **Privacy is about bad-behaved readers acquiring information from well-behaved tags.**
- **Nominal read range** These ranges represent the maximum distances at which a normally operating reader, with an ordinary antenna and power output, can reliably scan tag data.
- **Rogue scanning range:** When the range of a sensitive reader equipped with a powerful antenna—or antenna array—can exceed the nominal read range.
- **Tag-to-reader eavesdropping range** Once a reader has powered a tag, a second reader can monitor resulting tag emissions without itself outputting a signal.
- **Reader-to-tag eavesdropping range** Because readers transmit at much higher power than tags, they are subject to eavesdropping at much greater distances than tag-to-reader communications

Authentication

- Loosely speaking, RFID privacy concerns the problem of misbehaving readers harvesting information from well-behaving tags.
- RFID *authentication*, on the other hand, concerns the problem of **well-behaving readers harvesting information from misbehaving tags**, particularly counterfeit ones
- Basic RFID tags are vulnerable to simple counterfeiting attacks. Scanning and replicating such tags requires little money or expertise
- Unique numbering of objects can be a powerful anticounterfeiting tool.

Basic RFID tags

- Basic RFID tags, as defined, lack the resources to perform true cryptographic operations
- The lack of cryptography in basic RFID is a big impediment to security design.
- Cryptography, after all, is one of the lynchpins of data security.
- Even if some tags can do cryptography, pricing pressure is a strong countervailing force
- They will address security and privacy concerns using other, cheaper measures.

Privacy solutions basic tags: Killing and sleeping

- EPC tags address consumer privacy with a simple PIN protected kill command
- When an EPC tag receives a "kill" command from a reader, it renders itself permanently inoperative.
- It is envisioned that once RFID tags become prevalent on retail items, point-of-sale devices will kill the RFID tags on purchased items to protect consumer privacy, but it eliminates all of the post-purchase benefits of RFID for the consumer.
- Rather than killing tags at the point of sale, then, why not put them to "sleep," i.e., render them only temporarily inactive?
- Clearly, sleeping tags would confer no real privacy protection if any reader at all could "wake" them. However, some algorithms can prevent this situation.

Privacy solutions basic tags: Renaming

- To prevent RFID-tag tracking, it is necessary that tag identifiers be suppressed, or that they change over time.
- Relabeling can be done at the PoS but it needs to be changed over time.
- *Minimalist" cryptography: While high-powered devices like readers can relabel tags for privacy, tags can alternatively relabel themselves.*
- *Re-encryption: For example, using a single, universal key pair. A tag can send an encrypted message whose key is periodically changed. This doesn't mean that the tag has cryptographic capabilities at all.*
- Universal encryption. a universal re-encryption is a scheme in which a ciphertext can be digitally signed by a central authority, thereby permitting anyone to verify the authenticity of the associated plaintext, namely the tag identifier.

Privacy solutions basic tags: Proxying

- Rather than relying on public RFID readers to enforce privacy protection, consumers might instead carry their own privacy-enforcing devices for RFID. As already noted, some mobile phones include RFID functionality. They might ultimately support privacy protection.
- Examples:
 - TheWatchdog Tag monitors ambient scanning of RFID tags, and collects information from readers, like their privacy policies.
 - A Guardian (to use the first term) acts as a kind of personal RFID firewall. It intermediates reader requests to tags; viewed another way, the Guardian selectively simulates tags under its control. As a high-powered device with substantive computing power, a Guardian can implement sophisticated privacy policies, and can use channels other than RFID (e.g., GPS or Internet connections) to supplement ambient data

Privacy solutions basic tags: Distance measurement

- Some researchers have demonstrated that the signal-to-noise ratio of the reader signal in an RFID system provides a rough metric of the distance between a reader and a tag.
- They postulate that with some additional, low-cost circuitry a tag might achieve rough measurement of the distance of an interrogating reader.
- Researchers propose that this distance serve as a metric for trust.

Privacy solutions basic tags: Blocking

- Some researchers propose a privacy-protecting scheme that they call *blocking*.
- *Their scheme depends on the incorporation into tags of a modifiable bit called a *privacy bit*. A "0" *privacy bit* marks a tag as subject to unrestricted public scanning; a "1" bit marks a tag as "private."*
- Literature refers to the space of identifiers with leading "1" bits as a *privacy zone*. A *blocker tag* is a special RFID tag that prevents unwanted scanning of tags mapped into the privacy zone

Authentication

- EPC tags of the Class-1 Gen-2 type have no explicit anticounterfeiting features whatsoever.
- In principle, an attacker can simply skim the EPC from a target tag and program it into another, counterfeit tag—or simulate the target tag in another type of wireless device.
- Some tags already include anticounterfeiting solutions.
- Even if tags themselves do not carry on-board anticounterfeiting features, they can support physical anticounterfeiting mechanisms. Many forms of packaging today contain special, proprietary (and secret) dyes and other physical markers of uniqueness